SECURITY OF ONLINE GAMES

Why Online Games?

- Gaming is big business
  - Computer games for Microsoft platform totalled $6 billion (2005)
  - Half were retail games, half online games
  - Market for online poker: $300 million (2006)
- Online games are big
  - World of Warcraft: 11,5 million subscribers (2008)
  - 500K users online simultaneously

Why Online Games? (2)

- Game economies rival those of small countries
  - GDP of Everquest, $2266 per capita
  - More than India, Bulgaria, China, almost as wealthy as Russia
  - Wordwide annual sales of virtual goods: $900 million

Why Online Games? (3)

- Possibly sign of the future issues
  - Many parallel users
  - Users interacting with each other
  - Real-time processing
  - Rich content, rich client
  - Commonalities with Web 2.0

Early Games

- Arcade games – physical security
  - Protect the coinbox
  - Pinball: protect against tilting
- Standalone games – software piracy
  - Initially, quite serious
    - Quoting words from the manual
  - Later, more relaxed stance
  - Console games: consoles are cheap, games are expensive
    - Must protect against illegal game developers

Networked Games

- Multiplayer games
  - Only authentic copies are allowed to connect to server
  - Needs method to check correctness of key
  - Fight against unauthorized servers
- Online games
  - Pay by subscription
  - Some games also charge for client software (example: WoW)

Basic Attacks

- Cheating in card/board games
  - Collusion (poker, bridge)
  - Sandbagging
  - Escaping
- Collecting information
  - Player characteristics (poker)
  - Monster characteristics, probabilities (MMORPG)

Basic Attacks (2)

- Getting unfair information
  - Wall hack in shooters
  - Removing „fog of war”
  - Predicting poker hands

Basic Attacks (3)

- Breaking the rules of the game
  - Creating resources
    - Creating gold, items, forces
  - Changing game rules
    - Physics model
    - Invulnerability
    - Resource costs
  - Breaking policies in virtual worlds
  - Violating copyright (e.g. in Second Life)

Basic Attacks (4)

- Automating parts of the game
  - Bots
  - Playing poker
  - Aiming in shooters
  - Boring stuff in MMORPGs

Virtual Trading

- Game items are sold for real money
  - Gold
  - Equipment
  - Characters
- Usually using some mediating environment
  - Previously E-bay
  - Middlemen like IGE
  - Used by hackers/farmers to cash in
- You can also hire people to play for you

Farming

Farming (2)

- Not cheating as such
- Disrupts game economy/balance
  - Can cause inflation
- Usually farmers play the same copy of game in shifts

Technical Stuff

Architecture

- World is hosted on a server cluster
- Users connect using client software

- Game state
  - All the variables, all the files, state of all the components
- Some game state is managed by client
  - Usually because of bandwidth restrictions

Proxies

- Intercept (and modify) network traffic
  - Can also work on DLL level
- See state not shown in client
  - People behind walls
  - Properties of mobs, items
  - Fog of war

Proxies (2)

- Can modify data
- Aimbots
  - Build model of the game
  - Intercept firing command
  - Insert commands for turning
  - Insert firing command
  - Insert commands for turning back
- Talk to people not in the room

Aimbots

- Additional requirement: must be visually invisible
  - Think of a LAN party
- Cannot have perfect aim
  - Must use some randomization
  - However, some people are very accurate
- Call for Duty 4: view the kill from the viewpoint of the killer

Manipulate Process Memory

- Read game data
  - Sometimes, random events are precomputed
- Read video memory
  - Invisible objects

Breakpoints

- Normally used by debuggers for stepping through program
- Can be used to stop the game and manipulate state

Random Numbers

- Can you predict the next random event?

- Online poker games
  - Crack the PRNG
  - Game called randomize() before each shuffling
  - Milliseconds since midnight was used as a seed
  - Synchronize with server's time and try-guess the possible combinations

Lurking Bots

- Gather statistics
- MMORPG – where to find stuff
  - Who carries it?
  - Where is it found?
  - When will he drop it?
- Poker statistics
  - Find good tables
  - Player characteristics

Spyware

- Games include countermeasures to detect cheats
- Some games include spyware programs
  - WoW comes with Warden
- Often invasions of privacy
  - Poker software can take screenshot of the entire screen (all windows)
  - EFF classifies Warden as spyware
  - Online games often have interesting EULAs

Time and State Bugs

- Online worlds are fragmented
- For example, WoW runs 50,000 players per server
- Atomicity of actions at state boundaries
  - Logging out
  - Leaving party
  - Starting/stopping fighting
  - Transferring to other server

Race Conditions

- Can be used for exploiting non-atomic actions
- Lagging makes exploiting races easier
  - Example: create lag, give money to other person, log out
  - Client lag can be controlled by using proxy
  - Server lag can be created by botnet

State Machine Bugs

- Interactions of various spells
- Mutually exclusive spells
- Travelling bugs
  - Several travelling modifiers at once (flying, falling, running away)
  - Travel often controlled by the client software
    - Can just modify the x, y, z coordinates in client
    - Rate of fall controlled by the client

Manipulating the Client

- Modifying client-side game data
  - Modifying object coordinates
  - Modifying physical models
- Monitoring drops and respawns
  - Monsters drop stuff
  - Sometimes client software knows whether it will drop
  - Sometimes drop is controlled by client software
- Overcoming restrictions in user interface

Manipulating the Client (2)

- Reading and changing data
  - Data in memory
  - Data sent to video card (objects, walls, opaqueness)
  - Data sent to libraries (Directx, OpenGL)
- Scripting the client program
  - Sending user interface events (keyboard, mouse)
  - Read screen pixels
    - Determine health level, character state

Manipulating the Client (3)

- Manipulating DLLs
  - Replacing the network or graphics DLL
  - Example: wall hack
- Manipulating network traffic
  - Contains all the client state
  - Contains all the important events in server
  - Traffic often encrypted
    - Keys and algorithm are in the software

Manipulating the Client (4)

- Using kernel mode
  - Can do everything
  - Complete stealth
    - Safe from detection spyware

Changing the Game

- Modding
  - Usually replaces graphics
- Total conversion
  - Change everything
    - Including game rules, physics, ...
  - Example: Counter Strike – total conversion for Half-Life
- Custom clients
- Custom servers

Conclusion

- Side effects of massively parallel distributed processing
  - User interface issues
  - Trust issues
  - Bugs related to time and state